AMENDMENTS TO THE CLAIMS

Please cancel Claims 10, 22, 33, and 45.

Please amend Claims 1-5, 7-9, 11-17, 19-21, 23-28, 30-32, 34-40, 42-44, and 46 as follows:

1. (Currently amended) A process for storing and recovering security information stored on a first transportable memory device ~~smart card~~ that is used to uniquely access a client computer and secure logins into networks and Web sites, comprising the steps of:

providing a secure server;

creating a password and challenge question;

wherein said password is used to access said server if said first transportable memory device ~~smart card~~ is lost and said challenge question is used to confirm the user's identity when challenged while accessing said server without a transportable memory device ~~smart card~~;

retrieving ~~the~~ an ID number of said first transportable memory device ~~smart card~~ and other user and system specific information;

storing said first transportable memory device ~~smart card~~ ID and said other user and system specific information on said server;

providing access key creation means on said server for creating a first access key;

storing said first access key on said server; ~~and~~

providing configuration means for configuring said client to boot only if said first transportable memory device ~~smart card~~ is readable by said client or said first access key is entered[[.]] ;

wherein said access key creation means creates a second access key upon request by the user;

replacing said first access key with said second access key on said server; and

wherein said configuration means configures said client to boot if said second access key is entered, thereby replacing said first access key.

2. (Currently amended) The process of claim 1, wherein an emergency diskette is created and said client can boot using said diskette instead of said first transportable memory device ~~smart card~~.

3. (Currently amended) The process of claim 1, wherein the user accesses said server through another computer; wherein said server requires the user to log in; and wherein said server displays ~~said~~ a current access key to the user if said log in is correct.

4. (Currently amended) The process of claim 1, wherein the user enters ~~said first~~ a current access key into said client; and wherein said client boots in response to said ~~first~~ current access key.

5. (Currently amended) The process of claim 1, further comprising the steps of:

wherein the user requests that said server issue a second transportable memory device ~~smart card~~ to replace said first transportable memory device ~~smart card~~;

~~wherein the user makes said request through said client;~~

retrieving the ID number from said second transportable memory device ~~smart card~~;

replacing said first transportable memory device ~~smart card~~'s ID with said second transportable memory device ~~smart card~~'s ID on said server; and

wherein said configuration means configures said client to boot if said second transportable memory device ~~smart card~~ is readable, thereby replacing said first transportable memory device ~~smart card~~.

6. (Original) The process of claim 5, wherein said server requires the user to enter the proper user and/or other system specific information to validate said request.

7. (Currently amended) The process of claim 5, further comprising the step of:

wherein said access key creation means creates a ~~second~~ third access key;

replacing said first access key with said ~~second~~ third access key on said server; and

wherein said configuration means configures said client to boot if said ~~second~~ third access key is entered, thereby replacing said first access key.

8. (Currently amended) The process of claim 5, further comprising the step of:

providing morphing means for recreating ~~the~~ a personal computing environment stored on said first transportable memory device ~~smart card~~ onto said second transportable memory device ~~smart card~~.

9. (Currently amended) The process of claim 8, wherein said morphing means transfers ~~the~~ encryption and other rights of said first transportable memory device ~~smart card~~ to said second transportable memory device ~~smart card~~.

10. (Canceled)

11. (Currently amended) The process of claim 1, further comprising the step of:

providing automatic login means resident on said client for logging onto networks and/or Web sites, without the user's intervention, using the user's information stored on said first transportable memory device ~~smart card~~.

12. (Currently amended) A process for storing and recovering security information stored on a first transportable memory device ~~smart card~~ that is used to uniquely access a client computer, comprising the steps of:

providing a secure server;

retrieving the ID number of said first transportable memory device ~~smart card~~ and other user and system specific information;

storing said first smart card ID and said other user and system specific information on said server;

providing access key creation means on said server for creating a first access key;

storing said first access key on said server; ~~and~~

providing configuration means for configuring said client to boot only if said first transportable memory device ~~smart card~~ is readable by said client or said first access key is entered[[.]] ;

wherein said access key creation means creates a second access key upon request by the user;

replacing said first access key with said second access key on said server; and

wherein said configuration means configures said client to boot if said second access key is entered, thereby replacing said first access key.

13. (Currently amended) The process of claim 12, further comprising the step of:

creating a password and challenge question; and

wherein said password is used to access said server if said first transportable memory device ~~smart card~~ is lost and said challenge question is used to confirm the user's identity when challenged while accessing said server without a transportable memory device ~~smart card~~.

14. (Currently amended) The process of claim 12, wherein an emergency diskette is created and said client can boot using said diskette instead of said first transportable memory device ~~smart card~~.

15. (Currently amended) The process of claim 13, wherein the user accesses said server through another computer; wherein said server requires the user to log in; and wherein said server displays ~~said~~ a current access key to the user if said log in is correct.

16. (Currently amended) The process of claim 12, wherein the user enters ~~said first~~ a current access key into said client; and wherein said client boots in response to said ~~first~~ current access key.

17. (Currently amended) The process of claim 12, further comprising the steps of:

wherein the user requests that said server issue a second transportable memory device ~~smart card~~ to replace said first transportable memory device ~~smart card~~;

~~wherein the user makes said request through said client;~~

retrieving the ID number from said second transportable memory device ~~smart card~~;

replacing said first transportable memory device ~~smart card~~'s ID with said second transportable memory device ~~smart card~~'s ID on said server; and

wherein said configuration means configures said client to boot if said second transportable memory device ~~smart card~~ is readable, thereby replacing said first transportable memory device ~~smart card~~.

18. (Original) The process of claim 17, wherein said server requires the user to enter the proper user and/or other system specific information to validate said request.

19. (Currently amended) The process of claim 17, further comprising the step of:

wherein said access key creation means creates a ~~second~~ third access key;

replacing said first access key with said ~~second~~ third access key on said server; and

wherein said configuration means configures said client to boot if said ~~second~~ third access key is entered, thereby replacing said first access key.

20. (Currently amended) The process of claim 17, further comprising the step of:

providing morphing means for recreating ~~the~~ a personal computing environment stored on said first transportable memory device ~~smart card~~ onto said second transportable memory device ~~smart card~~.

21. (Currently amended) The process of claim 20, wherein said morphing means transfers ~~the~~ encryption and other rights of said first transportable memory device ~~smart card~~ to said second transportable memory device ~~smart card~~.

22. (Canceled)

23. (Currently amended) The process of claim 12, further comprising the step of:

providing automatic login means on said client for logging onto networks and/or Web sites, without the user's intervention, using the user's information stored on said first transportable memory device ~~smart card~~.

24. (Currently amended) A program storage medium readable by a computer, tangibly embodying a program of instructions executable by the computer to perform method steps for storing and recovering security information stored on a first transportable memory device ~~smart card~~ that is used to uniquely access a client computer, comprising the steps of:

providing a secure server;

creating a password and challenge question;

wherein said password is used to access said server if said first transportable memory device ~~smart card~~ is lost and said challenge question is used to confirm the user's identity when challenged while accessing said server without a transportable memory device ~~smart card~~;

retrieving the ID number of said first transportable memory device ~~smart card~~ and other user and system specific information;

storing said first transportable memory device ~~smart card~~ ID and said other user and system specific information on said server;

providing access key creation means on said server for creating a first access key;

storing said first access key on said server; ~~and~~

providing configuration means for configuring said client to boot only if said first transportable memory device ~~smart card~~ is readable by said client or said first access key is entered[[.]] ;

wherein said access key creation means creates a second access key upon request by the user;

replacing said first access key with said second access key on said server; and

wherein said configuration means configures said client to boot if said second access key is entered, thereby replacing said first access key.

25. (Currently amended) The method of claim 24, wherein an emergency diskette is created and said client can boot using said diskette instead of said first transportable memory device ~~smart card~~.

26. (Currently amended) The method of claim 24, wherein the user accesses said server through another computer; wherein said server requires the user to log in; and wherein said server displays ~~said~~ a current access key to the user if said log in is correct.

27. (Currently amended) The method of claim 24, wherein the user enters ~~said first~~ a ~~current~~ access key into said client; and wherein said client boots in response to said ~~first~~ current access key.

28. (Currently amended) The method of claim 24, further comprising the steps of:

wherein the user requests that said server issue a second transportable memory device ~~smart card~~ to replace said first transportable memory device ~~smart card~~;

~~wherein the user makes said request through said client;~~

retrieving the ID number from said second transportable memory device ~~smart card~~;

replacing said first transportable memory device ~~smart card~~'s ID with said second transportable memory device ~~smart card~~'s ID on said server; and

wherein said configuration means configures said client to boot if said second transportable memory device ~~smart card~~ is readable, thereby replacing said first transportable memory device ~~smart card~~.

29. (Original) The method of claim 28, wherein said server requires the user to enter the proper user and/or other system specific information to validate said request.

30. (Currently amended) The method of claim 28, further comprising the step of:

wherein said access key creation means creates a ~~second~~ third access key;

replacing said first access key with said ~~second~~ third access key on said server; and

wherein said configuration means configures said client to boot if said ~~second~~ third access key is entered, thereby replacing said first access key.

31. (Currently amended) The method of claim 28, further comprising the step of:

providing morphing means for recreating ~~the~~ a personal computing environment stored on said first transportable memory device ~~smart card~~ onto said second transportable memory device ~~smart card~~.

32. (Currently amended) The method of claim 31, wherein said morphing means transfers ~~the~~ encryption and other rights of said first transportable memory device ~~smart card~~ to said second transportable memory device ~~smart card~~.

33. (Canceled)

34. (Currently amended) The method of claim 24, further comprising the step of:

providing automatic login means resident on said client for logging onto networks and/or Web sites, without the user's intervention, using the user's information stored on said first transportable memory device ~~smart card~~.

35. (Currently amended) A program storage medium readable by a computer, tangibly embodying a program of instructions executable by the computer to perform method steps for storing and recovering security information stored on a first transportable memory device ~~smart card~~ that is used to uniquely access a client computer, comprising the steps of:

providing a secure server;

retrieving the ID number of said first transportable memory device ~~smart card~~ and other user and system specific information;

storing said first transportable memory device ~~smart card~~ ID and said other user and system specific information on said server;

providing access key creation means on said server for creating a first access key;

storing said first access key on said server; ~~and~~

providing configuration means for configuring said client to boot only if said first transportable memory device ~~smart card~~ is readable by said client or said first access key is entered[[.]] ;

wherein said access key creation means creates a second access key upon request by the user;

replacing said first access key with said second access key on said server; and

wherein said configuration means configures said client to boot if said second access key is entered, thereby replacing said first access key.

36. (Currently amended) The method of claim 35, further comprising the step of:

creating a password and challenge question; and

wherein said password is used to access said server if said first transportable memory device ~~smart card~~ is lost and said challenge question is used to confirm the user's identity when challenged while accessing said server without a transportable memory device ~~smart card~~.

37. (Currently amended) The method of claim 35, wherein an emergency diskette is created and said client can boot using said diskette instead of said first transportable memory device ~~smart card~~.

38. (Currently amended) The method of claim 36, wherein the user accesses said server through another computer; wherein said server requires the user to log in; and wherein said server displays ~~said~~ a current access key to the user if said log in is correct.

39. (Currently amended) The method of claim 35, wherein the user enters ~~said first~~ a current access key into said client; and wherein said client boots in response to said ~~first~~ current access key.

40. (Currently amended) The method of claim 35, further comprising the steps of:

wherein the user requests that said server issue a second transportable memory device ~~smart card~~ to replace said first transportable memory device ~~smart card~~;

~~wherein the user makes said request through said client;~~

retrieving the ID number from said second transportable memory device ~~smart card~~;

replacing said first transportable memory device ~~smart card~~'s ID with said second transportable memory device ~~smart card~~'s ID on said server; and

wherein said configuration means configures said client to boot if said second transportable memory device ~~smart card~~ is readable, thereby replacing said first transportable memory device ~~smart card~~.

41. (Original) The method of claim 40, wherein said server requires the user to enter the proper user and/or other system specific information to validate said request.

42. (Currently amended) The method of claim 40, further comprising the step of:

wherein said access key creation means creates a ~~second~~ third access key;

replacing said first access key with said ~~second~~ third access key on said server; and

wherein said configuration means configures said client to boot if said ~~second~~ third access key is entered, thereby replacing said first access key.

43. (Currently amended) The method of claim 40, further comprising the step of:

providing morphing means for recreating ~~the~~ a personal computing environment stored on said first transportable memory device ~~smart card~~ onto said second transportable memory device ~~smart card~~.

44. (Currently amended) The method of claim 43, wherein said morphing means transfers ~~the~~ encryption and other rights of said first transportable memory device ~~smart card~~ to said second transportable memory device ~~smart card~~.

45. (Canceled)

46. (Currently amended) The method of claim 35, further comprising the step of:

providing automatic login means resident on said client for logging onto networks and/or Web sites, without the user's intervention, using the user's information stored on said first transportable memory device ~~smart card~~.